IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

TRINITY BIAS, JAIME CARDENAS, CHRISTOPHER HOLMES, and ROBERT SHAW, individually and on behalf of all others similarly situated, Plaintiffs, v. ELEPHANT INSURANCE COMPANY, ELEPHANT INSURANCE SERVICES, LLC, and PLATINUM GENERAL AGENCY, INC. d/b/a APPARENT INSURANCE Defendants.	Civil Action No. 3:22-cv-00487-JAG **CLASS ACTION**

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

I. INTRODUCTION

Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), Plaintiffs Trinity Bias, James Cardenas, Christopher Holmes and Robert Shaw, individually and on behalf of the Class (collectively, "Plaintiffs") respectfully submit this opposition to the motion to dismiss filed by Defendants Elephant Insurance Company, Elephant Insurance Services, LLC, and Platinum General Agency, Inc. d/b/a Apparent Insurance (collectively, "Defendants" or "Elephant"). For all the reasons stated herein, Defendants' motion should be denied in its entirety.[1]

II. FACTUAL AND PROCEDURAL BACKGROUND

This Action arises out of a data breach which occurred between at least March 26, 2022 and April 1, 2022 at Elephant, an automobile insurance provider, that targeted the driver's license information of Elephant's customers, prospects, and even those with no relationship to Elephant at all (the "Unauthorized Data Disclosure" or "UDD"). ¶¶ 1, 25.[2] The UDD resulted in the unauthorized access to sensitive data belonging to approximately 2,762,687 putative Class Members (including Plaintiffs), who suffered out-of-pocket expenses and/or spent time to remedy or mitigate the effects of the attack. ¶ 2. In addition, Plaintiffs and Class Members are now faced with the present and continuing risk of identity theft caused by the compromise of their sensitive personal information, including their names, driver's license numbers, dates of birth, and other sensitive information provided in connection with an insurance plan, quote or application for an insurance plan (their "Personally Identifiable Information" or "PII"). *Id.*

As Plaintiffs allege, every year, millions of Americans have their most valuable personal information stolen and sold online because of data breaches and unauthorized data disclosures. ¶

[1] Should the Court disagree, Plaintiffs respectfully request leave to amend their complaint.
[2] All references to the Consolidated Class Action Complaint (ECF No. 18) are referred to with a paragraph symbol followed by the relevant paragraph numbers.

1. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies, including Elephant, still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data belonging to their customers or potential customers. *Id.* Cybercrime has been on the rise in recent years. ¶¶ 37-39. Tech experts have warned that fraudsters harvest driver's license numbers because they are highly valuable pieces of PII. ¶¶ 42-46. A driver's license can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate on the dark web for a stolen identity is about $1,200, and that a stolen or forged driver's license alone can sell for around $200. ¶ 44. "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, . . . use the information to craft curated social engineering phishing attacks, . . . [or use them] to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar." ¶ 46. Experts and authorities confirm that driver's license numbers are particularly useful to identity thieves for applying for unemployment and government benefits. ¶¶ 3, 44-50.

Despite the sensitivity of driver's license numbers, to boost sales numbers, insurers began to auto-populate them onto their online quoting platforms whenever any member of the public entered basic information such as name, address, and/or date of birth, and malicious actors took notice. The online websites of Geico, Farmers, USAA, Kemper, Metromile, and American Family were all targeted in 2021. ¶¶ 2, 3, 29, 35, 45-52. The New York State Department of Financial Services ("NYSDFS") issued two industry letters warning of this scheme. On February 16, 2021, NYSDFS stated it recently learned "of a systemic and aggressive campaign" in which cybercriminals targeted public-facing websites that offer instant online quotes to obtain unredacted driver's license numbers. ¶¶ 3 & n.1, 50. The NYSDFS followed up on March 30, 2021, noting

the "ongoing cybercrime campaign that is a serious threat to consumers," and urging insurers "to avoid displaying prefilled NPI on public facing websites." ¶ 57 n.39. Then, the NYSDFS recommended a series of security measures that would "combat this cybercrime" if implemented, including CAPTCHA to detect and block bots, improved access controls for Agent Portals, and eliminating accessibility to PII from the internet or agent portals. ¶ 58.

Even with these warnings, Elephant failed to take effective preventative measures, and between March 26, 2022 and April 1, 2022, similar to the long line of insurers listed above, it "identified unusual activity" on its "network," and "determined that certain consumer information may have been viewed on or copied from [its] network," including names and driver's license numbers – the exact same information that was viewed or copied in the "systematic and aggressive campaign" that had been noted in the industry over the previous 15 months. ¶¶ 26, 39. Elephant confirmed that at least part of the Data Disclosure was related to their quoting platform: "We have your information because you either are a current or previous Elephant Insurance customer *or we received your information as part of providing a quote for auto or other insurance coverage.*" ¶¶ 26-27 (emphasis added).

Just as with the long line of insurers who came before them, Elephant disclosed driver's license numbers of at least some members of the public who were not their customers. ¶¶ 26, 27, 95 (Plaintiff Holmes "had never heard of the Defendants"), ¶ 89 (Plaintiff Bias "has never purchased insurance from Elephant"). Thus, it is a reasonable inference that, at least where Elephant did not obtain PII from the Plaintiff or Class Member directly, malicious actors must have submitted Plaintiffs' and the Class's name on Elephant's quoting platform and Elephant disclosed their driver's license numbers back to the malicious actors there. Furthermore, Plaintiffs' Complaint specifically alleges that Elephant followed in its competitors' footsteps by providing

driver's license numbers to the malicious actors through its online quoting platform "between March 26, 2022, and April 1, 2022." ¶¶ 5, 26; *see also* ¶¶ 9, 55, 63-64, 78, 154, 156.

Plaintiffs were harmed by Elephant's failure to secure their PII. ¶¶ 81-131. Plaintiffs and the Class suffered a loss of privacy, incurred costs and spent significant time, effort and resources addressing the UDD, suffered anxiety, emotional distress, and other economic and non-economic losses, and are subject to a present and continuing risk of identity theft and fraud, as a result of the UDD. ¶¶ 81, 182. In addition, Plaintiff Cardenas has received notice that his driver's license is available for purchase on the dark web and spent time researching his options to respond to the UDD. ¶¶ 82-88. Plaintiff Holmes experienced an uptick in spam text and telephone calls, including unauthorized third-party spam attempting to sell insurance, received notice that his driver's license number was found on the dark web, and has spent time researching his options to respond to the UDD. ¶¶ 94-103. Finally, Plaintiff Shaw, a former Elephant customer, received notice that not only was his driver's license number compromised, so was his full name, date of birth, address, and any other sensitive PII Defendants had about him at the time of the breach – which could have included his Social Security number, telephone number, medical or disability information, and other motor vehicle records about his driving history. ¶¶ 105, 107.

III. PLAINTIFFS HAVE ARTICLE III STANDING

A. Plaintiffs have Demonstrated Article III Standing

To establish standing under Article III, a plaintiff must show three elements: injury-in-fact, causation, and redressability. *David v. Alphin*, 704 F.3d 327, 333 (4th Cir. 2017). Identifying an injury-in-fact is "a low threshold." *John v. Whole Foods Mkt. Grp., Inc.*, 858 F.3d 732, 736 (2d Cir. 2017). "The injury-in-fact requirement is 'very generous' to claimants. A plaintiff need only allege 'some specific, identifiable trifle of injury.'" *Pub. Interest Legal Found. v. Boockvar*, 370 F. Supp. 3d 449, 455 (M.D. Pa. 2019) (citations omitted); *see also Hutton v. Nat'l Bd. of Examiners*

in Optometry, Inc., 892 F.3d 613, 620 (4th Cir. 2018). A plaintiff must only establish a "realistic danger of sustaining a direct injury." *Peterson v. Nat'l Telcoms. & Info. Admin*. 478 F.3d 626, 632 (4th Cir. 2007) (quoting *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298 (1979)).

Elephant challenges only the injury-in-fact element of Article III standing and urges that Plaintiffs have "proffer[ed] nothing but speculative and hypothetical theories of injury" while demanding that Plaintiffs satisfy a standard beyond that which is required. Mot. at 5-6. All of Elephant's injury-in-fact challenges should be rejected.

B. Plaintiffs Have Alleged Concrete Injuries-in-Fact Resulting from the UDD

For Article III purposes, an injury in fact is "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (internal citations omitted). An injury in fact may be "actual or imminent," i.e., the harm need not yet materialize for a plaintiff to have standing. *Hutton*, 892 F.3d at 621. As the Third Circuit recently explained,

> That "actual or imminent" is disjunctive is critical: it indicates that a plaintiff need not wait until he or she has *actually* sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent. This is especially important in the data breach context, where the disclosure of the data may cause future harm as opposed to currently felt harm.

Clemens v. ExecuPharm Inc., 48 F.4th 146, 152 (3d Cir. 2022). To determine whether an injury is sufficiently imminent in the data breach context, the Third Circuit identified three factors to examine: (1) when "the data breach was intentional"; (2) when "the data was misused"; and (3) when "the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft." *Id*. at 153 (noting the factors are "useful guideposts" with no single factor dispositive"). Each is satisfied here. Plaintiffs allege that the UDD was targeted to acquire Plaintiffs' PII and explain the mechanism that the attacker used to intentionally acquire it. ¶¶ 1, 5.

Plaintiffs also allege their PII has been misused and published on the dark web for sale to fraudsters, ¶¶ 40-41, 83, 98, and that the driver's license information at issue here is desired by criminals precisely because of its use in committing fraud and identity theft. ¶¶ 29-53.

Moreover, the Fourth Circuit has noted that a risk of harm is imminent where the plaintiff alleges either actual misuse of data or that the cyberattack at issue targeted the data itself. *Beck v. McDonald*, 848 F.3d 262, 275-76 (4th Cir. 2017); *Hutton*, 892 F.3d at 622. Here, not only does the complaint allege that the object of the UDD was to acquire consumer data but also that two Plaintiffs have been informed that their driver's license information was published on the dark web following the UDD. ¶¶ 1, 5, 83, 98. Publication of personal information on the dark web is actual misuse sufficient to demonstrate Article III standing. *McCreary v. Filters Fast LLC*, 2021 WL 3044228, at *5 (W.D.N.C. July 19, 2021) ("These allegations of actual misuse bring the "actual and threatened harm" alleged by Plaintiffs "out of the realm of speculation and into the realm of sufficiently imminent and particularized harm."); *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, 2022 WL 3919685, at *5 (D. Md. Aug. 31, 2022) (citing to *McCreary* and publication of personal information published on the dark web as an example of actual misuse). For those Plaintiffs whose PII has not yet been published on the dark web, "the allegations of identity theft by other plaintiffs whose personal information was stolen makes the threatened injury sufficiently imminent," such that they have "established injury-in-fact based on the non-speculative imminent threat of identity theft." *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460 (D. Md. 2020); *In re Brinker Data Incident Litig.*, 2021 WL 1405508, at *5 (M.D. Fla. Apr. 14, 2021).

Defendant's reliance on *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) is misplaced and fails to discuss the distinction between *Beck* and the facts before this Court. *Beck* concerned two

different data breach cases which were consolidated for appeal. In one, a thief had stolen a laptop that incidentally housed PII. *Id*. at 267. In the other, several boxes of files containing patient data had gone missing and it was unclear whether those boxes had been stolen or simply misplaced. *Id*. at 268. In both those cases, there were no allegations that the actual data housed in the computer or file boxes had been the object of theft. On those facts, the Fourth Circuit upheld the District Court's dismissal orders because both cases were premised on the notion that because the laptop or files could not be located, the plaintiffs were exposed to increased risk of identity theft. *Id*. at 274. The *Beck* court engaged in an analysis of other court's rulings and noted that in each, the plaintiffs had alleged that the data was the object of the attack and because the data itself was sought, it was not speculative to assume that the data would be misused. *Id*. at 273.

Contrary to Defendant's position, the Fourth Circuit in *Beck* did not require that victims of a data breach must suffer actual misuse of their data before they could establish standing. *Id*. at 275. Rather, the Fourth Circuit noted that the district court required only allegations "sufficient to show that the threatened harm of future identity theft was 'certainly impending.'" *Id*. Plaintiffs have alleged not only that it is impending but that it has actually materialized. Elephant also argues Plaintiffs need to suffer out-of-pocket losses to satisfy the injury-in-fact element of standing, but again, that misapprehends the law. Neither a materialized injury nor an economic injury is necessary to demonstrate injury in fact. *McCreary*, 2021 WL 3044228, at *4 ("Fourth Circuit precedent does not support Defendant's argument that Plaintiffs must suffer out-of-pocket loss to establish an injury-in-fact.") (citing to *Hutton*, 892 F.3d at 622). Accordingly, Plaintiffs' injuries are non-speculative, imminent, and actual and thus confer Article III standing.

C. Plaintiffs' Mitigation Efforts Were Reasonable and Necessary

Elephant next accuses the victims of the UDD of manufacturing standing, argues that Plaintiffs' mitigation efforts are self-inflicted harm, and that absent out of pocket losses, Plaintiffs'

mitigation efforts are not injuries in fact. Mot. at 9-10. However, when coupled with allegations of actual misuse of personal information, the time spent mitigating the consequences of the UDD suffices to demonstrate a non-speculative injury in fact. *Hutton*, 892 F.3d at 622 ("[T]he Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists."); *In re Marriott*, 440 F. Supp. 3d at 459 ("out-of-pocket costs and time spent to mitigate the harms also constituted injury-in-fact") (citing to *Hutton*); *Stamat*, 2022 WL 3919685, at *5, 7; *Cotter v. Checkers Drive-In Restaurants, Inc.*, 2021 WL 3773414, at *6 (M.D. Fla. Aug. 25, 2021). Accordingly, because Plaintiffs' mitigation efforts were predicated on a non-speculative and imminent threat of injury, Plaintiffs "incurred concrete damages as a proximate result of the Data Breach." *In re GE/CBPS*, 2021 WL 3406374, at *9 (S.D.N.Y. Aug. 4, 2021) (collecting cases). Finally, Elephant cites no case holding Plaintiffs must incur out of pocket costs to demonstrate injury-in-fact with respect to their mitigation efforts. Rather, as the cases cited above note, time or money spent mitigating the consequences of a data breach suffice to demonstrate injury *See, e.g.*, *In re Marriott*, 440 F. Supp. 3d at 459. As noted by the Fourth Circuit in *Hutton*, "the Supreme Court long ago made clear that "[i]n interpreting injury in fact ... standing [is] not confined to those who [can] show economic harm." 892 F.3d at 622 (quoting *United States v. Students Challenging Regulatory Agency Procs.*, 412 U.S. 669, 686 (1973)); *see also Pender v. Bank of Am. Corp.*, 788 F.3d 354, 366 (4th Cir. 2015).

D. Emotional Injuries are Concrete Injuries in Fact

Elephant next argues that the emotional injuries Plaintiffs suffered as a result of their data being compromised and in the hands of criminals are not sufficiently concrete. Mot. at 10. Contrary to Elephant's argument, emotional injuries are concrete injuries sufficient to confer standing. *Clemens*, 48 F.4th at 156 ("[I]f the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress . . . the plaintiff has alleged a concrete

injury."); *Stamat*, 2022 WL 3919685, at *7 (D. Md. Aug. 31, 2022) ("Emotional injuries may suffice for Article III standing purposes"). The Supreme Court of the United States also expressed as much in *TransUnion LLC v. Ramirez*, holding that the risk of future harm, coupled with injury "such as emotional injury" may suffice to demonstrate Article III standing.141 S. Ct. 2190, 2211 (2021).

While Elephant complains that Plaintiffs have alleged only the existence of these injuries and nothing more, Plaintiffs have alleged not only their injuries but have also pleaded facts that demonstrate such a reaction is reasonable given the harm to which they have been subjected. ¶¶ 29-53, 101, 114, 120-22, 125-27, 129-31, 182. Accordingly, Defendants' arguments that Plaintiffs have failed to meet their pleading standard are unavailing.

E. Plaintiffs have Adequately Pleaded the Diminution in Value of their Personal Information.

Elephant also argues that the diminution in value of Plaintiffs' personal information as a result of the UDD is "an entirely speculative and hypothetical injury that does not provide Plaintiffs with standing." Mot. at 11. Courts routinely find that a loss of value in personal information resulting from a data breach is a concrete injury sufficient to confer standing. *See In re Marriott.*, 440 F. Supp. 3d at 462 (collecting cases); *see also Opris v. Sincera Reprod. Med.*, 2022 WL 1639417, at *8 (E.D. Pa. May 24, 2022) ("[T]he alleged loss of value to their PII . . . further supports that they suffered damages as a result of [Defendants'] negligence."); *McCreary*, 2021 WL 3044228, at *6 (diminished value of personal information demonstrates standing). There is no requirement that Plaintiffs demonstrate the existence of a consumer marketplace in which they could sell their personal information. As the *In re Marriott* court explained:

> [T]he value of consumer personal information is not derived solely (or even realistically) by its worth in some imagined market place where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the

> consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check.

440 F. Supp. 3d at 462. Other courts agree the value of PII is axiomatic. *Smallman v. MGM Resorts Int'l*, 2022 WL 16636958, at *6 (D. Nev. Nov. 2, 2022) (dark web presence sufficient); *Klein v. Facebook, Inc.*, 580 F. Supp. 3d 743, 803 (N.D. Cal. 2022).

Plaintiffs pled that the PII here is of high value to criminals, desired because it can be used to commit fraud and identity theft, and that compromise of this PII impedes them from enjoying everyday life activities. ¶¶ 29-53, 120-22, 125-27. This is enough; to require more defies the practical reality that PII clouded by misuse is of a lesser value than that which is not.

F. Plaintiffs Sufficiently Allege Entitlement to Injunctive Relief.

Finally, Elephant argues that Plaintiffs lack standing to seek injunctive and declaratory relief. Mot. at 12. Elephant first argues that Plaintiffs have failed to demonstrate that they are at an imminent and substantial risk of future harm as a result of the UDD. Mot. at 12. Once again, Elephant ignores that Plaintiffs' allegations that their information was targeted and subsequently posted for sale on the dark web suffice to demonstrate an imminent risk of harm. ¶¶ 83, 98; *see Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals.... Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966 (7th Cir. 2016), (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015); ("It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is 'sooner or later to make fraudulent charges or assume those consumers' identities.'")). As the DC Circuit in the OPM data breach case opined, "[i]t hardly takes a criminal

mastermind to imagine how [personal] information could be used to commit identity theft." *In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 56 (D.C. Cir. 2019).

While Elephant argues that the nature of the PII at issue does not present a credible risk to Plaintiffs, this ignores that the information has been published on the dark web, the specific harms that can result from the misuse of driver's license information, and the value placed on it by those who would inflict those harms. ¶¶ 1, 29-53, 83, 98, 125-27. Simply put, if the information compromised in the data breach did not present a risk to Plaintiffs there would be no need for criminals to target and attempt to sell it or for Elephant to admonish victims of the UDD to guard against identity theft and fraud and provide credit monitoring services. ¶¶ 28, 129-30; *Galaria*, 663 F. App'x at 388 ("Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year.").

Elephant next argues that even if the information compromised in the UDD presents an immediate risk of injury, Plaintiffs have failed to identify the nature of injunctive relief that would prevent such harm. Mot. at 13. But Elephant ignores that Plaintiffs seek a declaration concerning the inadequacy of Defendant's security practices and injunctive relief to address those inadequacies and ensure Defendant's implementation of reasonable security measures. ¶ 254. Notably, Elephant has not identified the steps it took in response to the UDD, and while it continues to maintain Plaintiffs' PII even if they are not Elephant customers, Plaintiffs cannot rely on Elephant's assurances, both in its privacy policy with respect to data security and that it has rectified the issues that led to the UDD. ¶¶ 8, 26, 106, 249-253. Absent an order compelling Elephant to implement reasonable data security measures, Plaintiffs are at a present and certainly imminent risk that the PII maintained by Elephant will be targeted and acquired once again. This demonstrates Plaintiffs' entitlement to injunctive and declaratory relief. *See, e.g.*, *In re Adobe Sys.,*

Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014); *Smallman*, 2022 WL 16636958, at *13, 18.

G. Controlling Fourth Circuit Precedent Establishes That Plaintiffs Have Article III Standing to Bring Their DPPA Claims for Damages.

The Fourth Circuit recently definitively confirmed that plaintiffs who allege a DPPA violation "have alleged a legally cognizable privacy injury" and thus "have Article III standing to pursue claims for damages." *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 922 (4th Cir. 2022). Elephant fails to mention this controlling precedent anywhere in its brief, including in the eight pages dedicated to its argument that Plaintiffs lack Article III standing. Mot. at 5-13.

In *Garey*, the Fourth Circuit explains Article III standing based on the DPPA in light of the Supreme Court's recent decision in *TransUnion LLC v. Ramirez*, 141 S.Ct. at 2204. First, the Fourth Circuit correctly notes that "[b]ecause standing is a threshold jurisdictional question" that asks whether a plaintiff has a "legally cognizable injury," an appeals court must address it first, and *de novo*. *Garey*, 35 F.4th at 921 (internal quotation omitted). Second, the Fourth Circuit explains that "Congress may, of course, 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'" *Id.* (citing *Lujan*, 504 U.S. at 57). Third, the Fourth Circuit explains that "simply [] pleading a statutory violation" will not establish Article III standing unless that violation constitutes "a concrete injury." *Id.* (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). Fourth, as explained in *TransUnion*, "plaintiffs proceeding under a statutory cause of action [such as the DPPA] can establish a cognizable injury by identifying a close historical or common-law analogue . . . for which courts have 'traditionally' provided a remedy." *Id.* (internal quotations omitted). Finally, the Fourth Circuit holds: "[c]onsistent with *TransUnion*, [standing exists under the DPPA] *because plaintiffs' alleged harms*

are closely related to the invasion of privacy, which has long provided a basis for recovery at common law." *Id.* (emphasis added) (internal quotations omitted).

In *Garey*, the Fourth Circuit compares the DPPA to the Telephone Consumer Protection Act, 47 U.S.C. § 227, which it also found "protects particular and concrete privacy interests" and thus "plainly satisfies the demands of Article III." *Id.* at 922 (citing *Krakauer v. Dish Network, LLC*, 925 F.3d 643, 652-54 (4th Cir. 2019)). The Court explains that "our inquiry focuses on types of harms protected at common law," and a cognizable injury need not meet "the elements of common law torts, piece by piece." *Id.* (internal citations omitted). Because "[a]t bottom, the DPPA is aimed squarely at 'the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone,'" the Plaintiffs have Article III standing to pursue claims for damages. *Id.* (citing William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 389 (1960); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)). As to the amount of damages: "The DPPA provides for liquidated damages of $2,500 if a plaintiff cannot prove actual damages greater than that amount," and thus "it follows that proof of actual damages is not necessary for an award of liquidated damages under the DPPA." *Id.* at 922, n.4 (cleaned up). Thus, in *Garey* the Fourth Circuit established by controlling precedent that Plaintiffs have Article III standing to bring their claims for damages under the DPPA, and Elephant's failure to cite this case invites reversible error.

H. Plaintiffs Also Have Article III Standing Under the DPPA to Bring Their Claims for Injunctive and Declaratory Relief.

In *Garey*, the Fourth Circuit also noted that "a plaintiff must demonstrate standing separately for each form of relief sought," and "a plaintiff can satisfy the injury-in-fact requirement for prospective relief either by demonstrating a sufficiently imminent injury in fact or by demonstrating an ongoing injury. . . ." *Id.* at 922 (cleaned up) (citing *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs (TOC), Inc.*, 120 S.Ct. 693 (2000)). In *TransUnion*, the Supreme Court

explained that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." 141 S. Ct. at 2210 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013); *see also Bates v. UPS, Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (standing inquiry for injunctive relief requires plaintiffs to demonstrate a suffered or threatened 'concrete and particularized' legal harm, coupled with a 'sufficient likelihood that [they] will again be wronged in a similar way'") (citation omitted). Where, as here, Plaintiffs have alleged that Elephant has obtained their DPPA-protected PII, including driver's license numbers, and disclosed or redisclosed it to malicious actors via its online quoting platforms, *even where Plaintiffs are not Elephant's customers*, Plaintiffs will continue to be exposed by this practice, and are entitled to seek injunctive relief to protect themselves from its continuation. As one court explained in a similar case to this one against insurer Farmers:

> [H]ackers were able to obtain Plaintiff's PII from Defendants' online quoting system despite Plaintiff not being a customer of Defendants. Plaintiff argues that without injunctive relief requiring Defendants to remedy the deficiencies in their security measures, Plaintiff's PII could be 'obtained again in the same unauthorized manner.' Plaintiff therefore faces a 'real and immediate threat' of further disclosure of his PII, which remains in the hands of Defendants. . . . . Accordingly, at this stage of the litigation, Plaintiff has adequately alleged standing to seek injunctive and declaratory relief.

Stallone v. Farmers Group, Inc., 2022 WL 10091489 at *9 (D. Nev. Oct. 15, 2022) (internal citations omitted).[3] As another court explained in two other similar cases against insurers USAA

[3] *See In re Ambry Genetics Data Br. Litig.*, 567 F. Supp. 3d 1130, 1141 (C.D. Cal. 2021) (plaintiff had standing for injunctive relief where plaintiff asserted requiring defendants to implement and maintain reasonable security measures was needed to prevent future data breaches); *In re Yahoo! Inc. Customer Data Sec. Br. Litig.*, 2017 WL 3727318, at *31 (N.D. Cal. Aug. 30, 2017) (plaintiffs had standing to pursue injunctive relief to mitigate the threat of future data breaches when defendants possessed class PII); *In re Adobe*, 66 F. Supp. 3d at 1223 (same); *Leonard v. McMemamins*, 2022 WL 4017674, at *5-6 (W.D. Wash. Sept. 2, 2022) (same).

and Travelers, where, under these circumstances, a plaintiff seeks injunctive relief to require a defendant to "implement certain specific security protocols," an injunction "will serve the public interest," and "may proceed." *In re: USAA Data Security Litig.*, 2022 WL 3346527, at *11-12 (S.D.N.Y. Aug. 12, 2022); *see also Rand v. The Travelers Indemnity Co.*, 2022 WL 15523722, at *11 (S.D.N.Y. Oct. 27, 2022).[4]

IV. PLAINTIFFS ADEQUATELY STATE A CLAIM FOR RELIEF

A. The Standard of Review

To survive a Rule 12(b)(6) motion to dismiss, a complaint need only allege sufficient facts to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). Courts must "assum[e] that all the [factual] allegations in the complaint are true." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Rule 12(b)(6) does not countenance [] dismissals based on a judge's disbelief of a complaint's factual allegations." *Id.* at 556. The complaint must be construed liberally, and any allegations or reasonable inferences arising therefrom must be interpreted in the light most favorable to the plaintiff. *Id.* at 554-56.

B. Plaintiffs Adequately Plead a Violation of the DPPA by Alleging a "Knowing Disclosure" on Elephant's Online Quoting Platform.

Elephant argues that Plaintiffs have failed to state a claim under the DPPA. Mot. at 14-18. However, rather than analyze this question based on Plaintiffs' actual allegations, as required for

[4] In *Garey*, plaintiffs lacked standing for injunctive relief because the defendants there—attorneys who obtained car accident reports to solicit personal injury cases—were only accused of "obtaining" Plaintiffs' personal information in violation of the DPPA, not of disclosing or redisclosing that PII. But there, defendants had already "obtained" the PII in question and required a speculative future car crash and exact replication of unusual circumstances, which the Fourth Circuit found too speculative. 35 F.4th at 923. The opposite is true here: the allegations demonstrate Elephant discloses or rediscloses any person's driver's license when a malicious actor submits that person's name, address and/or date of birth, even when the submitted person has no prior contact with, or hasn't even heard of, Elephant. ¶ 95. This practice if not enjoined subjects the Class to continuous harm any time a hacker decides to exploit the quoting platform.

a motion to dismiss under Rule 12(b)(6), Elephant characterizes those allegations dismissively as "distractions" and "a maneuver." Ultimately, Elephant attempts to contradict Plaintiffs' allegations factually: "That is not the type of data breach Elephant suffered." *Id.* at 18. Factual disputes cannot be resolved at the motion to dismiss phase, and even if they could, Elephant has not offered any actual facts to support its contradiction. Elephant's argument merely underscores that this case must proceed to discovery to develop a factual record.

The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724(a). Additionally, the DPPA provides a second layer of protection to drivers' privacy by regulating "the resale and *redisclosure* of drivers' personal information by private persons who have obtained that information from a state DMV." *Reno v. Condon*, 528 U.S. 141, 146 (2000) (emphasis added). Under the DPPA, disclosure or redisclosure of such information is prohibited unless made "for a purpose permitted by an exception listed in 1 of 14 statutory subsections." *Id.*at 145 n.1 (citing § 2724(b)(1)-(14)). "Any person who rediscloses or resells personal information from DMV records must for five years, maintain records identifying to whom the records were disclosed and the permitted purpose for the resale or redisclosure." *Id.* at 146 (citing § 2724(c)).

In enacting the DPPA, Congress was motivated by its concern "that personal information collected by States in the licensing of motor vehicle drivers was being released—even sold—with resulting loss of privacy for many persons."*Maracich v. Spears*, 570 U.S. 48, 51-52 (2013) (citing 18 U.S.C. §§ 2721-2725). The DPPA permissible use exceptions are exceptions to the default rule that entities are prohibited from disclosing, using, or obtaining personal information. *Id*. at 60.

Elephant's sole argument that Plaintiffs fail to state a claim under the DPPA centers on its proposed interpretation of the term "knowingly disclose." *See* Mot. at 15-18. Elephant argues that because unauthorized third parties accessed the data, Elephant could not have taken voluntary action and therefore did not "knowingly disclose" Plaintiffs' PII. *Id.* at 14-15. This takes an impermissibly narrow view of the term "knowingly disclose." Plaintiffs allege that Elephant "intentionally configured and designed [its] online insurance quoting platform to generate responses . . .that included [auto-populated] personal information ('PI')," which resulted in the disclosure of Plaintiffs' driver's license numbers to malicious actors. ¶¶ 5, 7. These allegations constitute a knowing disclosure under the DPPA. Courts consistently find that a "knowing disclosure is merely a disclosure made voluntarily." *See Senne v. Village of Palatine*, 695 F.3d 597, 603 (7th Cir. 2012) ("Voluntary action, not knowledge of illegality or potential consequences" is sufficient under the DPPA); *Enslin v. The Coca-Cola Company*, 136 F. Supp. 3d 654, 670 (E.D. Pa. 2015) ("A knowing disclosure of PDI requires the defendant take some voluntary action to disclose the information.") (internal quotations and citation omitted); *see also Pichler v. UNITE*, 542 F.3d 380, 396 (3d Cir. 2008) (rejecting the argument that "civil liability requires a defendant knowingly obtain or disclose personal information for a use the defendant knows is impermissible"). Accordingly, "knowing" is a low bar under the DPPA.

Under this standard, Elephant certainly took voluntary action and knowingly disclosed Plaintiffs' PII, including their driver's license numbers. Elephant intentionally configured its online quote system so that any member of the public could fill in information and receive a quote. ¶¶ 5, 9, 26, 27, 55, 63, 64, 78, 154, 156. This meant that anyone with a few basic bits of data could use Elephant's system to retrieve sensitive information, including driver's license numbers and other data. Indeed, through Elephant's voluntary configuration of its online quote system,

unauthorized third parties were allowed to take Plaintiffs' driver's license numbers and dates of birth. ¶ 7. Thus, Elephant "knowingly disclose[d] or otherwise ma[de] available" Plaintiffs' personal information from motor vehicle records, in direct violation of the DPPA. *See Senne*, 695 F.3d at 602. ("In our view, attaching the terms 'or otherwise make available' to the term 'disclose' leaves little doubt about the breadth of the transactions Congress intended to regulate."); *see also Welch v. Theodorides-Bustle*, 677 F. Supp. 2d 1283, 1286-87 (N.D. Fla. 2010) (upholding DPPA claim where the defendants did not deny that plaintiff's personal information was "made available on the internet" where "an internet user can access the information for any or no reason—or on a whim" and concluding that "alleging specifically that there was a disclosure, and alleging generally that there was no proper purpose for the disclosure, is enough").

Two district courts recently denied motions to dismiss in cases involving nearly identical facts and held that when insurance companies disclose driver's license numbers on their online quoting platforms this constitutes "knowing disclosure" under the DPPA. Plaintiffs in a case involving the USAA insurance company alleged that the insurer "designed its website" so that "an individual seeking a quote for any of USAA's insurance policies could do so by first creating a USAA account, which requires providing 'minimal information,'" and "once the account is made, the USAA member would then receive an online quote form pre-filled with personally identifiable information ('PII') . . . including the member's driver's license number." *In re: USAA*, 2022 WL 3348527, at *1. In denying the motion to dismiss the DPPA claim, the court explained that "a 'knowing disclosure' is a disclosure made voluntarily, not necessarily one made with 'knowledge of illegality or potential consequences.'" *Id.*, at *7 (citing *Senne*). The court concluded that "USAA's voluntary decision to automatically pre-fill its quote forms with driver's license numbers constitutes a 'knowing disclosure' of personal information." *Id.*, at *7 (citing 18 U.S.C. § 2724(a)).

The court further held that "USAA reasonably should have known its pre-filling of driver's license numbers would disclose that protected information directly to cybercriminals for impermissible purposes." *Id.*

Another district court agreed in a case involving the Farmers insurance company: "As in *In re USAA*, the Court finds that Defendants made a voluntary decision to automatically pre-populate its online quote forms with individuals' driver's license numbers upon receiving minimal personal information. Although Defendants were not necessarily aware that this practice would result in the instant UDD, the Court finds that Defendants' decision to configure the online quoting platform was a 'knowing disclosure' of PII." *Stallone*, 2022 WL 10091489, at *10. Like these other cases, this Court should find the same.

The cases Elephant cites are readily distinguishable. Mot. at 16. In *Allen v. Vertafore*, the defendant did not take any knowing and voluntary action leaving the plaintiffs' PII susceptible to outside parties, as Plaintiffs allege Elephant has here. *Allen v. Vertafore, Inc.*, 2021 WL 3148870, at *4 (S.D. Tex. June 14, 2021), *aff'd* 28 F.4th 613 (5th Cir. 2022). Rather, the defendant in *Vertafore* merely left information on unsecured servers inadvertently, servers that nonetheless were within its control. *Id.* As such, no data was knowingly disclosed to anyone outside the company. *Id.* This is clearly distinguishable from the allegations here, that Elephant intentionally configured a system through which DPPA-protected PII was disclosed to outside third parties on its online quoting platform. ¶¶ 5, 9, 26-27, 55, 63-64, 78, 154, 156.

Elephant's reliance on *Enslin v. The Coca-Cola Co.* is similarly misplaced. In *Enslin*, a defendant stored the plaintiffs' PII in unencrypted form on various laptops. 136 F. Supp. 3d at 658. Over six years, fifty-five laptops containing the plaintiffs' PII were stolen by a defendant's employee. The court held that the defendant did not knowingly disclose the plaintiffs' PII, as the

defendant's only voluntary action was putting the plaintiffs' PII on its own privately-held laptops, which were not shared with anyone outside the company or displayed to the public. *Id.* at 671. By contrast, Elephant affirmatively configured a system through which the public could, and did, access Plaintiffs' PII without Plaintiffs' authorization. ¶¶ 5, 9, 26-27, 55, 63-64, 78, 154, 156.

Plaintiffs here make similar allegations as the *In re USAA* and *Farmers* plaintiffs, and adequately allege that Elephant's decision to pre-fill driver's license numbers on its quote forms knowingly disclosed PII in violation of the DPPA. ¶¶ 5, 9, 26, 27, 55, 63, 64, 78, 154, 156.

C. Plaintiffs Adequately State a Claim for Negligence

In Virginia, the essential negligence claim elements "are (1) the identification of a legal duty of the defendant to the plaintiff, (2) a breach of that duty; and (3) injury to the plaintiff proximately caused by the breach." *Talley v. Danke Med., Inc.*, 179 F.3d 154, 157 (4th Cir. 1999) (citation omitted).[5] Defendants here argue only that Plaintiffs failed to allege actual damages—despite the authority holding otherwise. Plaintiffs' negligence claims are adequately pled.

Plaintiffs allege they are subject to an increased risk of identity theft and fraud because of the UDD, have suffered loss of privacy, and have spent significant time, effort, and resources addressing the UDD. ¶ 81. These damages are recognized as appropriate to maintain a negligence claim in data breach cases—where the stolen information was sensitive and plaintiff(s) alleges misuse. *See Clemens*, 48 F.4th at 159 (negligence damages sufficiently pled where information was stolen, misused, and published to the dark web, "and the sensitive information is the type that could be used to perpetrate identity theft or fraud"); *In re USAA*, 2022 WL 3348527, at *6 (driver's license numbers are sufficiently sensitive information because of the high risk of identity theft or

[5] The negligence claim elements are substantially identical in every jurisdiction. *Compare Kroger Co. v. Elwood*, 197 S.W.3d 793, 794 (Tex. 2006); *First Springfield Bank & Tr. v. Galman*, 188 Ill. 2d 252, 256 (Ill 1999); *Keiswetter v. State*, 373 P.3d 803, 805 (Kan. 2016).

fraud if disclosed.); *Stallone*, 2022 WL 10091489, at *5 (driver's licenses sufficiently similar to Social Security numbers because their value is derived from their immutability). Plaintiffs allege their information was sensitive (¶¶ 6, 54), stolen (¶ 7), Plaintiffs Cardenas' and Holmes's driver's license numbers were actually posted to the dark web (¶¶ 83, 98), and the sensitive information was misused (¶ 9).

First, the imminent risk of identity theft is plausible and more than just speculative where a plaintiff alleges her/his personally identifiable information was stolen, posted online, and misused. *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 403 (E.D. Va. 2020). This holding is consistent with other courts that routinely find the damages claimed from ongoing risk of identity theft are not speculative. *See In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021) ("Given the colossal amount of sensitive data stolen . . . and the unequivocal damage that can be done with this type of data, we have no hesitation in holding that Plaintiffs adequately alleged that they face a 'material' and 'substantial' risk of identity theft"); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 302 (2d Cir. 2021); *Galaria*, 663 F. App'x at 388; *Stallone*, 2022 WL 10091489, at *6; *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 686-687 (D.S.C. 2021) (allegations of risk of extortion, unauthorized disclosure of PII, risk of future identity theft or fraud, and time and money spent mitigating exposure sufficient at pleading stage). There is nothing speculative about Plaintiffs' harm because (a) Defendants warn of the risk of identity fraud; (b) the driver's licenses of Plaintiffs Cardenas and Holmes are already for sale on the dark web; and (c) Plaintiff Holmes is receiving increased spam texts and calls since the disclosure. ¶¶ 83, 97-98.

Second, Defendants argue time spent responding to the UDD is not a sufficient injury to support a negligence claim. This is incorrect; numerous courts have held time spent responding to

a data breach is a recognized damage for a negligence claim. *See In re Solara Medical Supplies Data Breach Litig.*, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020) (collecting cases) (citing *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019)*; In re Cap. One*, 488 F. Supp. 3d at 390 (time spent on mitigation efforts adequate damages). Elephant cites *In re SuperValu, Inc. Customer Data Sec. Breach Litig.*, 2018 WL 1189327 (D. Minn. Mar. 7, 2018); that court's decision relied on the fact that sensitive information was not stolen, and courts distinguish *SuperValu* in cases involving PII to hold the claim sufficiently pled. *See In re: Netgain Tech., LLC*, 2022 WL 1810606, at *5 (D. Minn. June 2, 2022). Here, the data at issue is sensitive—specifically Plaintiffs' and Class Members' driver's license numbers—and Plaintiffs have spent time dealing with the UDD. For example, Plaintiff Holmes spent approximately 8 hours as of the time of filing of the Complaint reviewing documents—at Defendants' direction—to mitigate his losses. ¶¶ 5, 99. The other Plaintiffs have also spent time responding to the UDD by reviewing credit and financial documents for indications of fraud and/or identity theft. ¶¶ 84, 90, 113.

Defendants argue that Plaintiffs must wait until they suffer financial loss to have a viable claim for damages. Courts reject this premise and state that "[t]o require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact." *Stallone,* 2022 WL 10091489, at *6; *accord Clemens,* 48 F.4th at 159 (plaintiffs "cannot be required to wait until [they have] experienced actual identity theft or fraud before [they] can sue"); *see also Clapper,* 568 U.S. at 414 n.5.

The cases cited by Defendants are out of district and factually distinguishable. For example, in *Bohnak v. Marsh & McLennan Cos., Inc.*, 580 F. Supp. 3d 21 (S.D.N.Y. 2022) and *Everhart v. Colonial Pipeline Co.*, 2022 WL 3699967 (N.D. Ga. July 22, 2022) plaintiffs alleged sensitive

information was included in the data breach, but did not allege their information had been posted to and/or available on the dark web or otherwise misused. Here, Plaintiffs allege precisely how the exposure of their driver's license numbers creates a substantial threat of identity theft (*see, e.g.*, ¶¶ 2, 29-31, 35), specifically allege Plaintiffs Cardenas's and Holmes's driver's license numbers are now posted to the dark web, and that the information is being used for spam calls and texts—including third parties posing as debt collectors attempting to collect fictional debts, making *Bohnak* and *Everhart* factually distinguishable. ¶¶ 83, 97, 98.

Plaintiffs' allegations of an ongoing risk of identity theft and fraud, the posting of Plaintiffs Cardenas's and Holmes's driver's license numbers on the dark web, and loss of privacy resulting from the theft of their PII, that required expenditure of significant time, effort, and resources sufficiently support the survival of their negligence claim.

D. Plaintiffs Adequately State a Claim for Negligence *Per Se*

To pursue a claim of negligence *per se* in Virginia, a plaintiff must show: (1) "the defendant violated a statute enacted for public safety," (2) that plaintiffs "belong to the class of persons for whose benefit the statute was enacted," (3) "the harm that occurred was of the type against which the statute was designed to protect," and (4) "the statutory violation [was] a proximate cause of" their injury. *Collett v. Cordovana*, 772 S.E.2d 584, 589 (Va. 2015).[6] Plaintiffs meet this bar.

Here, the DPPA provides a statutory basis for Plaintiffs' negligence *per se* claim (¶ 187), and the DPPA is a statute enacted for public safety. *Gaston v. LexisNexis Risk Sols., Inc.*, 483 F. Supp. 3d 318, 333 (W.D.N.C. 2020). When faced with a similar claim on analogous facts, the court in *In Re: USAA Data Security Litigation* held:

[6] Negligence *per se* elements are substantially similar in other jurisdictions. *Compare First Springfield Bank & Tr.*, 188 Ill. 2d at 256 ("a plaintiff must show that (1) she belongs to the class of persons that the statute was designed to protect; (2) her injury is of the type that the statute was designed to prevent; and (3) the violation proximately caused her injury.")

> (i) the DPPA "was designed to protect a class of persons" comprising individuals whose PII has been misused or disclosed for an impermissible purpose; (ii) plaintiffs plausibly allege they became a part of that class as a result of [defendant's] data breach; and (iii) the criminal use of plaintiffs' PII is the "type of harm [that] in fact occurred as a result of [the DPPA's] violation," [defendant's] duty of care to plaintiffs and its breach of that duty are conclusively established upon proof that the statute was violated.

2022 WL 3348527, at *10. Here, Plaintiffs' allegations are similar, and satisfy the four elements by alleging (1) Defendants violated the DPPA—a statute enacted for public safety; (2) Plaintiffs and Class Members are within the class of persons the DPPA was designed to protect; (3) the harm that has occurred is the type the DPPA was intended to protect against; and (4) Defendants' violation of the DPPA directly and proximately caused Plaintiffs' injuries. ¶¶ 187-190.

Courts have also held negligence *per se* claims adequately pled based on alleged violations of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, also pled by Plaintiffs here. *In re Cap. One*, 488 F. Supp. 3d at 407; *In re Marriott*, 440 F. Supp. 3d at 479. Whether specific state laws impact the applicability of the FTC Act as an additional underlying statutory basis of Plaintiffs' negligence *per se* cause of action however is not properly resolved on a motion to dismiss. *See In re: Netgain*, 2022 WL 1810606, at *7 (choice of law analysis on a motion to dismiss premature as "courts generally decline to conduct a choice-of-law analysis prior to discovery"); *see also Harris Rutsky & Co. Ins. Services, Inc. v. Bell & Clements Ltd.*, 328 F.3d 1122, 1135 (9th Cir. 2003) (denial of jurisdictional discovery abuse of discretion when it may "demonstrate facts sufficient to constitute a basis for jurisdiction").

As discussed above, Plaintiffs plausibly allege a DPPA violation, and Plaintiffs adequately plead a violation of Section 5 of the FTC Act. The negligence *per se* claim should proceed.

E. Plaintiffs Adequately State a Claim for Unjust Enrichment

Defendants benefit from the retention and use of Plaintiffs' and Class Members PII. Unjust enrichment is predicated on "the receipt of a benefit and the unjust retention of the benefit at the

expense of another." *In re Cap. One*, 488 F. Supp. 3d at 411.[7] Where there is no express contract between parties, such as between Plaintiffs Cardenas, Bias, and Holmes and the Defendants, courts have held that failing to secure data "can give rise to an unjust enrichment claim" where a defendant accepts the benefits of plaintiffs' data at plaintiffs' expense "by not implementing adequate safeguards," making it "inequitable and unconscionable" for that defendant to retain the benefit while "leaving the plaintiff party to live with the consequences." *Id.* at 412.

Plaintiffs allege Defendants profited by using Plaintiffs' and Class Members' PII to market their services and facilitate providing online quotes to potential clients, thus leading to more customers and profits—a monetary benefit. Specifically, Defendants used Plaintiffs' and Class Members' PII for sales, marketing, and profitable purposes. ¶¶ 153, 201. Plaintiffs allege Defendants acknowledge on their website that they received a benefit from Plaintiffs' and Class Members' PII by using the PII for marketing its products to Plaintiffs, Class Members, and the general public. ¶ 193. Defendants were also "enriched at Plaintiffs' expense when [Defendants] chose to cut costs by not implementing security measures to protect Plaintiffs' PII." *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017); ¶ 204. Here, as evidenced by the details of the process leading to the UDD and as discussed previously, Defendants failed to provide reasonable and adequate security despite being aware of the sensitivity of the information it was using. ¶¶ 194, 197. Elephant leaves Plaintiffs and Class Members to live with the risks and consequences of identity theft and fraud. Therefore, Plaintiffs properly plead unjust enrichment.

Defendants' arguments regarding Plaintiff Shaw also fail. Plaintiff Shaw alleges he conferred a benefit on the Defendants by way of insurance premiums, that Defendants appreciate

[7] Substantively, unjust enrichment is fairly consistent across jurisdictions, all based on this same justification. *See In re Cap. One*, 488 F. Supp. 3d at 411 (citing California, Florida, New York, Texas, Virginia, and Washington state court cases).

or acknowledge the benefit, use the premiums to pay data security costs, that Defendants failed to implement adequate security to protect his PII—as evidenced by Defendants' alleged auto-populating a public-facing webpage with PII—and that Defendants should not be allowed to retain customers' money because Defendants failed to implement industry standard security measures. ¶¶ 5, 104, 193, 197, 201. This is all that is required at the pleading stage. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012).

While federal courts do not yet have a uniform analysis of unjust enrichment claims in data breach class actions where plaintiffs allege a portion of the monies received by defendant were supposed to be spent on data security, as one court put it, "we struggle to see how else [defendant] could support an adequate data security apparatus without profits derived from customer purchases." *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 538-540 (M.D. Pa. 2021). Additionally, while Elephant cites *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 765-766 (C.D. Ill. 2020), *Perdue* is distinguishable because that court based its decision on the fact plaintiff purchased goods and failed to allege the products were defective or dangerous. Here, Plaintiffs allege that customers, such as Plaintiff Shaw, purchased insurance from Defendants, Defendants understood and appreciated the benefits of the transaction and use of the PII collected, Defendants should have used a portion of the profits from insurance premiums to cover the costs of reasonable and adequate security, Plaintiff Shaw and the customer Class Members were overcharged for insurance services by Elephant, who failed to provide reasonable and adequate data security, and it would be unjust for Defendants to retain the benefits. ¶¶ 104, 193, 202, 204.

F. Plaintiffs Adequately Allege their State Claims

Elephant argues that Plaintiffs Holmes and Cardenas' Texas Deceptive Trade Practices and Consumer Protection Act ("TDTPA") claim fails because they do not allege reliance on or harm from Elephant's false, misleading or deceptive conduct. Mot. at 23. This is inaccurate. As Elephant

notes, Plaintiffs adequately allege that Elephant engaged in false, misleading, or deceptive acts and practices through their inadequate data security and misrepresentations and omissions that they would protect Plaintiffs' PII. ¶ 209. Defendants knew of and were obligated to reveal these facts because defendants with sub-standard security practices have a duty to reveal those facts to their consumers. *In re Cap. One*, 488 F. Supp. 3d at 427; *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1251 (D. Colo. 2018) (quotation omitted); *see also In re Adobe*, 66 F. Supp. 3d. at 1229. Plaintiffs plead reliance by explaining that they would have acted differently had they known the true state of Defendants' security practices. ¶¶ 195, 218. This is adequate at the pleadings stage. *See*, *e.g.*, *Marriott*, 440 F. Supp. 3d at 489; *In re Arby's Rest. Grp. Litig.*, 317 F. Supp. 3d 1222, 1225 (N.D. Ga. 2018); *Gordon*, 344 F. Supp. 3d at 1251. Plaintiffs need not have read Elephant's privacy policies. *See In re Yahoo!, Inc. Cust. Data Sec. Br. Litig*., 313 F. Supp. 3d 1113 (N.D. Cal. 2018). Plaintiffs adequately explain harm elsewhere; the TDTPA claim survives.

Elephant argues only that Plaintiff Bias's and the Illinois subclass's Illinois Consumer Fraud Act ("ICFA") claim fails because Plaintiff Bias failed to allege actual pecuniary harm, allegedly necessary to maintain an ICFA claim. However, Plaintiff Bias clearly alleged actual losses that constitute pecuniary harm, most especially lost time spent researching her options to respond to the theft of her driver's license number and in reviewing her credit and financial documents in order to detect fraud. ¶ 90. Such lost time as a result of Elephant's failures to protect her PII constitutes actual pecuniary harm under the ICFA. "[T]he value of one's own time needed to set things straight is a loss from an opportunity-cost perspective." *Dieffenbach v. Barnes & Noble, Inc.,* 887 F.3d 826, 828-29 (7th Cir. 2018); *see also Perdue*, 455 F. Supp. 3d at 761; *In re Arthur J. Gallagher Data Breach Litig*, 2022 WL 4535092, at *6 (N.D. Ill. Sept. 28, 2022). Plaintiff Bias's claim survives.

Elephant makes a single argument to dismiss Plaintiff Bias's and the Illinois subclass's Illinois Uniform Deceptive Trade Practices Act ("ILUDTPA") claims, which is based on the misrepresentation that Plaintiff Bias's only allegations of future harm are a threat of future identity theft and fraud as a result of Defendants' failures to protect her PII that resulted in the data breach. Mot. at 25. However, this is simply not true. Among many other harms alleged by Plaintiff Bias and the Illinois subclass, are "the current and ongoing risk to their PI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Bias's and Illinois Subclass Members' PI in Defendants' continued possession." ¶ 243(f). Such risks are a risk of future harm as a result of Elephant's misleading trade practices, including Elephant's failure to implement and maintain reasonable security and privacy measures and misrepresenting that Elephant would protect Plaintiff Bias's and the Illinois Subclass's PII. *See* ¶ 239. As Elephant acknowledges, plaintiffs can maintain a claim under the IUDTPA if they are "likely to be damaged in the future by the defendant's misleading trade practices." *Id.* (quoting *Perdue,* 455 F. Supp. 3d at 773).

Perdue is instructive. There, the court dismissed the IUDTPA claim because the only future harms alleged resulted from the data breach at issue and the only security risks at issue had been cured. *See id.* at 773 ("[T]he Court cannot stop hackers from using their information in the future. Additionally, Plaintiffs acknowledge that Defendant has 'removed the malware and implemented enhanced security measures.'"). Here, Plaintiffs allege ongoing future harms as a result of Elephant's deceptive trade practices, and that Elephant's continued possession and use of Plaintiff Bias's PII in an unsecure way while continuing to falsely represent that it holds such data securely is an ongoing harm with forward-looking damages such that an injunction under the IUDTPA is necessary to cure. As such, Elephant's motion should be denied.

G. Plaintiffs Adequately State a Claim for Declaratory and Injunctive Relief

Elephant only challenges Plaintiffs' claims for declaratory judgment and injunctive relief on the basis that the forward-looking injunctions sought would not prevent the UDD which has already happened. But as clearly and plainly alleged, Plaintiffs and the Class face impending future harms based on Defendants' continued failures to maintain adequate security, including the risk of future data breaches based on Elephant's unwillingness to properly secure their PII. *See, e.g.,* ¶ 253 ("Plaintiffs remain at ongoing and imminent risk that further compromises of their PI will occur in the future."), ¶¶ 254-257. Courts regularly allow declaratory judgment and injunctive relief claims to proceed in this instance. *See, e.g., In re Cap. One,* 488 F. Supp. 3d at 414-415; *Baker v. Parkmobile, LLC,* 2022 WL 3704003, at *10 (N.D. Ga. Aug. 19, 2022); *In re: The Home Depot, Inc., Cust. Data Security Breach Litig.*, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016). Here, Plaintiffs allege their PII remains in Elephant's possession, and that Elephant is still at risk of causing substantial harm due to its continuing inadequate security practices, justifying injunctive relief. ¶¶ 253-57. Defendants' motion should be denied.

V. THE COURT SHOULD NOT STRIKE COMPLAINT ALLEGATIONS

Motions to strike under Rule 12(f) are "generally viewed with disfavor "because striking a portion of a pleading is a drastic remedy and because it is often sought by the movant simply as a dilatory tactic.'" *Waste Management Holdings, Inc. v. Gilmore*, 252 F.3d 316, 347 (4th Cir. 2001) (quoting 5A Wright Miller, *Fed. Prac. & Proc.* § 1380, 647 (2d ed. 1990)). To overcome this high hurdle, movants must show they are entitled to this "drastic remedy" by showing that the portion of the pleading that is proposed stricken "might confuse the issues in the case" or give rise to "unfair prejudice." *LBCMT 2007-C3 Urbana Pike, LLC v. Sheppard*, 302 F.R.D. 385, 386 (D. Md. 2014). Elephant's baseless assertions that the paragraphs at issue here are unrelated to the claims

raised by Plaintiffs, despite their clear relationship to establishing duty, foreseeability, breach of duty, and damages, simply do not justify the imposition of this "drastic remedy" and certainly, inaccurate and inapposite as they are, constitute nothing more than a dilatory tactic by Elephant. Their argument to strike twenty-one paragraphs from the complaint should instead be seen as incredulity at the truth of Plaintiffs' assertions and a misunderstanding of how Plaintiffs' allegations help establish Defendants' knowledge of, and the foreseeability of, the risks to which they chose to subject Plaintiffs, Defendants' duties to Plaintiffs and the class, breach of those duties, and the ongoing risks of harm and damages to Plaintiffs and the Class as a result.

One set of the challenged paragraphs shows that Elephant was on notice to the risk of cybercrime, including from direct warnings issued to Elephant and the insurance industry by government authorities, or point to Elephant's negligence and failures to protect Plaintiffs' and the Class's PII despite clear knowledge of its need to improve security. ¶¶ 37-39, 47-50, 59. Another shows the level of security government and industry authorities have established as being the minimum necessary security precautions for businesses, like Elephant, to follow to adequately protect the PII they collect, and which Elephant should have maintained; these paragraphs act to show Elephant's duties to Plaintiffs and the Class. ¶¶ 65-68, 70. Paragraphs 120 and 126 both show the ongoing risks of harm and future damages faced by the Class. ¶¶ 120, 126.

Finally, Paragraphs, 41-42, 44-46, and 53 all speak to the value of the PII compromised here to cybercriminals and establish a likelihood that Plaintiffs will face harm for years to come due to Elephant's failures, which supports their damages claims as well as a conclusion that Elephant has a duty to protect their PII. ¶¶ 41-42, 44-46, 53. They should not be stricken.

VI. CONCLUSION

Plaintiffs respectfully request that the Court deny Defendants' motion to dismiss.

Dated: November 14, 2022

Respectfully submitted,

By: /s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, VA 22314
Telephone: (888) 987-9991
swebster@websterbook.com

By: /s/ Lee A. Floyd
Lee A. Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (804) 351-9170
Lee@bbtrial.com
Justin@bbtrial.com

Kevin Biniazan, VSB #92019
Jeffrey A. Breit, VSB #18876
BREIT BINIAZAN, P.C.
Towne Pavilion Center II
600 22nd Street, Suite 402
Virginia Beach, Virginia 23451
Telephone: (757) 622-6000
Facsimile: (757) 670-3939
Jeffrey@bbtrial.com
Kevin@bbtrial.com

Interim Class Liaison Counsel

Kate M. Baxter-Kauf*
Karen Hanson Riebel*
Maureen Kane Berg**
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com

M. Anderson Berry*
Gregory Haroutunian**

R. Michael Wells, Jr.**
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
mwells@justice4you.com

Interim Class Counsel

Gayle M. Blatt*
P. Camille Guerra*
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com
camille@cglaw.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

David K. Lietz**
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

**pro hac vice*
***pro hac vice forthcoming*

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on this day, November 14, 2022, I caused a true and correct copy of the foregoing motion to be filed with the Clerk of the Court for the Eastern District of Virginia via the Court's CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matters.

Dated: November 14, 2022 */s/ Lee A. Floyd*